CLAIMS:

What is claimed is:

1. A method in a computer system for generating a certificate for use only within said computer system to authenticate operations internal to said computer system, said method comprising the steps of:

establishing a security subsystem within said computer system;

establishing a master key pair including a master private key and a master public key;

storing said master private key in a protected storage within said security subsystem, wherein said master private key is inaccessible outside of said security subsystem;

supplying a target public key;

requesting generation of a self-verifying certificate;

prompting a user for an authentication code in response to a request for generation of said certificate; and

generating a self-verifying certificate utilizing said target public key and said master key pair only in response to a correct entry of said authentication code, said certificate used only internally within said computer system.

2. The method according to claim 1, further comprising the step of storing said authentication code in said security subsystem.

3. The method according to claim 2, further comprising the step of prohibiting an alteration of said authentication code after said authentication code is stored in said security subsystem.

4. The method according to claim 2, further comprising the step of prohibiting access to said authentication code to devices outside of said security subsystem after said authentication code is stored in said security subsystem.

5. The method according to claim 1, further comprising the step of determining a certificate identifier after a correct entry of said authentication code, said certificate identifier uniquely identifying said certificate.

6. The method according to claim 1, further comprising the steps of:

said security subsystem generating security data for said certificate after a correct entry of said authentication code;

said security subsystem hashing said security data;

said security subsystem encrypting said security data utilizing said master private key to create a signature; and

said security subsystem appending said signature to said security data to create said certificate.

7. The method according to claim 1, further comprising the step of storing said certificate along with a certificate identifier in said computer system.

8. The method according to claim 1, further comprising the steps of

receiving information within an appended certificate;

requesting authentication of a signature included within said appended certificate;

said security subsystem reading said master public key from said protected storage;

said security subsystem using said master public key to decrypt said signature; and

said security subsystem determining whether said signature is authentic.

9. A computer system for generating a certificate for use only within said computer system to authenticate operations internal to said computer system, said method comprising the steps of:

a security subsystem within said computer system;

a master key pair including a master private key and a master public key;

a protected storage within said security subsystem for storing said master private key, wherein said master private key is inaccessible outside of said security subsystem;

a target public key;

said computer system including a CPU executing code for requesting generation of a self-verifying certificate;

said computer system including a CPU executing code for prompting a user for an authentication code in response to a request for generation of said certificate; and

a self-verifying certificate generated utilizing said target public key and said master key pair only in response to a correct entry of said authentication code, said certificate used only internally within said computer system.

10. The system according to claim 9, further comprising said security subsystem for storing said authentication code.

11. The system according to claim 10, further comprising said computer system including a CPU executing code for prohibiting an alteration of said authentication code after said authentication code is stored in said security subsystem.

12. The system according to claim 10, further comprising said computer system including a CPU executing code for prohibiting access to said authentication code to devices outside of said security subsystem after said authentication code is stored in said security subsystem.

13. The system according to claim 9, further comprising a certificate identifier being determined after a correct entry of said authentication code, said certificate identifier uniquely identifying said certificate.

14. The system according to claim 9, further comprising:

said security subsystem for generating security data for said certificate after a correct entry of said authentication code;

said security subsystem for hashing said security data;

said security subsystem for encrypting said security data utilizing said master private key to create a signature; and

said security subsystem for appending said signature to said security data to create said certificate.

15. The system according to claim 9, further comprising said certificate being stored along with a certificate identifier in said computer system.

16. The system according to claim 9, further comprising:

said computer system including a CPU executing code for receiving information within an appended certificate;

said computer system including a CPU executing code for requesting authentication of a signature included within said appended certificate;

said security subsystem for reading said master public key from said protected storage;

said security subsystem for using said master public key to decrypt said signature; and

said security subsystem for determining whether said signature is authentic.